ORDER FOR SUPPLIES OR SERVICES

PAGE 1 OF 70

1. CONTRACT/PURCH ORDER/AGREEMENT NO.	2. DELIVERY ORDER/CALL NO.	3. DATE OF ORDER/CALL (YYYYMMMDD)	4. REQUISITION/PURCH REQUEST NO.	5. PRIORITY
N0017819D7566	N6449820F3002	2020SEP28	1300885553	Unrated

6. ISSUED BY CODE N64498

NAVAL SURFACE WARFARE CENTER PHILA
NSWCPD
Philadelphia, PA 19112-1403

7. ADMINISTERED BY *(If other than 6)* CODE

SCD: C

8. DELIVERY FOB
- ☐ DESTINATION
- ☐ OTHER *(See Schedule if other)*

9. CONTRACTOR CODE 1GUU1 FACILITY 009997602

NAME AND ADDRESS
EHS Technologies Corporation
1221 N. Church Street, Suite 106
Moorestown, NJ 08057

10. DELIVER TO FOB POINT BY *(Date) (YYYYMMMDD)*
SEE SCHEDULE

11. X IF BUSINESS IS
- ☒ SMALL
- ☐ SMALL DISAD-VANTAGED
- ☐ WOMEN-OWNED

12. DISCOUNT TERMS
Net 30 Days WAWF

13. MAIL INVOICES TO THE ADDRESS IN BLOCK
SEE SECTION G

14. SHIP TO CODE

SEE SECTION F

15. PAYMENT WILL BE MADE BY CODE N68732

DFAS Norfolk
1837 Morris Street, Suite 1401
Norfolk, VA 23511-3431

MARK ALL PACKAGES AND PAPERS WITH IDENTIFICATION NUMBERS IN BLOCKS 1 AND 2.

16. TYPE OF ORDER

- DELIVERY/CALL ☒ This delivery order/call is issued on another Government agency or in accordance with and subject to terms and conditions of above numbered contract.
- PURCHASE ☐ Reference your furnish the following on terms specified herein.

ACCEPTANCE. THE CONTRACTOR HEREBY ACCEPTS THE OFFER REPRESENTED BY THE NUMBERED PURCHASE ORDER AS IT MAY PREVIOUSLY HAVE BEEN OR IS NOW MODIFIED, SUBJECT TO ALL OF THE TERMS AND CONDITIONS SET FORTH, AND AGREES TO PERFORM THE SAME.

EHS Technologies Corporation			
NAME OF CONTRACTOR	SIGNATURE	TYPED NAME AND TITLE	DATE SIGNED *(YYYYMMMDD)*

☐ If this box is marked, supplier must sign Acceptance and return the following number of copies:

17. ACCOUNTING AND APPROPRIATION DATA/LOCAL USE

SEE SCHEDULE

18. ITEM NO.	19. SCHEDULE OF SUPPLIES/SERVICES	20. QUANTITY ORDERED/ ACCEPTED*	21. UNIT	22. UNIT PRICE	23. AMOUNT
	SEE SCHEDULE				

*If quantity accepted by the Government is same as quantity ordered, indicate by X. If different, enter actual quantity accepted below quantity ordered and encircle.

24. UNITED STATES OF AMERICA
BY: 09/29/2020 CONTRACTING/ORDERING OFFICER

25. TOTAL $7,053,092.10

26. DIFFERENCES

27a. QUANTITY IN COLUMN 20 HAS BEEN

☐ INSPECTED ☐ RECEIVED ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT EXCEPT AS NOTED:

b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	c. DATE *(YYYYMMMDD)*	d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE	28. SHIP. NO.	29. D.O. VOUCHER NO.	30. INITIALS
	☐ PARTIAL ☐ FINAL	32. PAID BY	33. AMOUNT VERIFIED CORRECT FOR
f. TELEPHONE NUMBER / g. E-MAIL ADDRESS	31. PAYMENT		34. CHECK NUMBER
36. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT.	☐ COMPLETE ☐ PARTIAL ☐ FINAL		
a. DATE *(YYYYMMMDD)* / b. SIGNATURE AND TITLE OF CERTIFYING OFFICER			35. BILL OF LADING NO.

37. RECEIVED AT	38. RECEIVED BY *(Print)*	39. DATE RECEIVED *(YYYYMMMDD)*	40. TOTAL CONTAINERS	41. S/R ACCOUNT NUMBER	42. S/R VOUCHER NO.

Section C - Description/Specifications/Statement of Work

STATEMENT OF WORK

for

Research, Development, Test, & Evaluation (RDT&E) Network, Navy Marine Corp Intranet (NMCI), and Next Generation Enterprise Network (NGEN) Support

1.0 INTRODUCTION

1.0.1 The Naval Surface Warfare Center Philadelphia Division (NSWCPD) is a Department of Defense entity responsible for research and development, test and evaluation, engineering and fleet support organization for the Navy's ships, submarines, military watercraft and unmanned vehicles. This requirement is for NSWCPD Code 104, which is the responsible Information Technology Operations Division of NSWCPD's Research, Development, Test & Evaluation (RDT&E) Network.

1.0.2 This contract is for non-personal services. It does not create employment rights with the U.S. Government whether actual, inherent, or implied

1.0.3 Government / Contractor Relationship

(a) The services to be delivered under this Task Order are non-personal services and the parties recognize and agree that no employer-employee relationship exists or will exist under the task order between the Government and the Contractor's personnel. Therefore, it is in the best interest of the Government to provide both parties a full understanding of their respective obligations.

(b) The Contractor employees shall identify themselves as Contractor personnel by introducing themselves or being introduced as Contractor personnel and displaying distinguishable badges or other visible identification for meetings with Government personnel. In addition, Contractor personnel shall appropriately identify themselves as Contractor employees in telephone conversations and in formal and informal written correspondence

(c) Contractor personnel under this task order shall not engage in any of the inherently Governmental functions listed at FAR Subpart 7.5 or DFARS Subpart 207.5.

(d) Employee Relationship:

1) The services to be performed under this Task Order do not require the Contractor or its personnel to exercise personal judgment and discretion on behalf of the Government. Rather the Contractor's personnel will act and exercise personal judgment and discretion on behalf of the Contractor.

2) Rules, regulations, directives, and requirements that are issued by the U. S. Navy and NSWCPD under its responsibility for good order, administration, and security are applicable to all personnel who enter a Government installation or who travel on Government transportation. This is not to be construed or interpreted to establish any degree of Government control that is inconsistent with a non-personal services contract.

(e) Inapplicability of Employee Benefits: This task order does not create an employer-employee relationship. Accordingly, entitlements and benefits applicable to such relationships do not apply.

(f) Notice. It is the Contractor's, as well as the Government's, responsibility to monitor task order activities and notify the Contracting Officer if the Contractor believes that the intent of this Section has been or may be violated.

1) The Contractor should notify the Contracting Officer in writing within three (3) calendar days from the date of any incident that the Contractor considers to constitute a violation of this Section. The notice should include the date, nature, and circumstances of the conduct; the name, function, and activity of each Government employee or Contractor official or employee involved or knowledgeable about such conduct; identify any documents or substance of any oral communication involved in the conduct; and the estimate in time by which the Government must respond to this notice to minimize cost, delay, or disruption of performance.

2) The Contracting Officer will, within five (5) calendar days after receipt of notice, respond to the notice in writing. In responding, the Contracting Officer will either:

(i) Confirm the conduct is in violation and when necessary direct the mode of further performance,

(ii) Countermand any communication regarded as a violation,

(iii) Deny that the conduct constitutes a violation and when necessary direct the mode of further performance, or

(iv) In the event the notice is inadequate to make a decision, advise the Contractor what additional information is required, and establish the date by which it should be furnished by the Contractor.

1.1 BACKGROUND

1.1.1 The Information Technology Operations Division (Code 104) of the Naval Surface Warfare Center, Philadelphia Division (NSWCPD) provides IT services and long-term support for (1) the operation, maintenance, and enhancement of the Research, Development, Test, & Evaluation (RDT&E) Network hardware and cabling, (2) Computer Operations and Production Control, (3) Navy Marine Corp Intranet (NMCI) administration and Next Generation Enterprise Network (NGEN) administration, and (4) Information Technology Customer Support, at its Philadelphia, PA site. This Task order will be in support of NSWCPD's Information Technology Division, Code 104

1.2 SCOPE OF WORK

1.2.1 The contractor shall provide all technical services outlined and necessary for the proper functioning of the day to day IT and administrative operations of the Code 104 Information Technology Operations Division. The Task Areas so identified are:

1) Network Operation and Maintenance Services;

2) Engineering;

3) Design/Installation of Network Extensions and Enhancements Services:

4) Telecommunications Services;

5) Server/Desktop Administration;

6) Information Management (IM), User Support;

7) Video Telecommunications (VTC) / Audio Visual (AV);

8) Continuity of Operations Plan (COOP);

9) High Performance Computing;

10) Operations and Production Control;

11) Documentation of Network Infrastructure;

12) NMCI/NGEN Support;

13) Departmental NMCI Coordination and Support;

14) Administrative and graphics Support for NSWCPD Code 104 ;

15) Cybersecurity;

16) Information Technology Support/Coordination (ITC);

17) Data Base Administration;

18) Software Development.

1.2.2 Under these task areas, the contractor shall supplement Code 104's Cybersecurity Workforce (CSWF), its engineers and support staff by performing routine maintenance and management of critical DON cyber systems and adjoining administrative functions. These duties to include but not limited to: Information Assurance (IA) compliance- certification and accreditation (C&A), Data At Rest (DAR) security, Information Assurance Vulnerability Management (IAVM)- Security Technical Implementation Guides (STIGs), Security Requirements Guide (SRGs), Virtual Private Network (VPN) management, electronic spillages and incident handling, media transfer agents, network operations, system operations, security systems, VTC support, IA policy- DoD, DON & NAVSEA, DON Application and Database Management System (DADMS) and DoD Information Technology Portfolio Repository (DITPR).

2.0 APPLICABLE DOCUMENTS

The Contractor shall reference and utilize the latest version of acquisition regulations, business practices, and RMF document requirements contained in relevant DoD/DoN instructions. The most current versions of the following documents form a part of this SOW to the extent speci?ed, herein.

2.1 Department of Defense Information Technology Risk Management Framework memo concerning DON IMPLEMENTATION OF THE RISK MANAGEMEI FRAMEWORK (RMF) FOR DOD INFORMATION TECHNOLOGY (IT)

2.2 DoD Instruction 8510.01 of 12 March 2014, Risk Management Framework (RMF) for DoD Information Technology (IT)

2.3 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Guide for Applying the Risk Management Framework to Federal Information System of February 2010, as amended

2.4 Committee on National Security Systems Instruction 1253 of March 27, 2014, Security Categorization and Control Selection for National Security Systems a amended

2.5 NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, of 30 April 2013, as amended

2.6 DoD Instruction 8500.01 of 14 March 2014, DoD Cybersecurity

2.7 DoD 8570.01-M Information Assurance Workforce Improvement Program

These documents can be referenced at www.doncio.navy.mil

3.0. REQUIREMENTS

This task order requires that the Contractor shall accomplish work as described in Paragraphs 3.1 through 3.18.

Contractor shall document project execution in accordance with Department of Navy requirements and within time constraints, which includes project scheduling and resource loading. Contractor shall conduct on-site personnel management of its employees, as well as partnering with Government project managers to ensure all key activities and actions are captured, scheduled, and risks identified and mitigated.

TASK AREA REQUIREMENTS

3.1 Task area 1: Network Operation and Maintenance Services

3.1.1 The contractor shall provide the necessary labor and material to provide operation and maintenance services for a RDT&E network that supports data, voice, and video applications. The network employs Ethernet, optical, and wireless technologies. The services include operating, maintaining, securely configuring, patching, troubleshooting and diagnostic testing of network equipment and network routing protocols to determine the cause of network problems/failures and repairing those problems/failures in a timely manner. Troubleshooting and repair services are required on all the network equipment which includes, but is not limited to, file servers, blade servers, communications servers, routers, bridges, switches, firewalls, Virtual Private Networks (VPN), power supplies, modems, Uninterrupted Power Supply (UPSs), network interface cards, and cable plant (twisted pair and fiber). Approximately 2,000 devices are connected and communicate on the network. Contractor shall:

- Troubleshoot - identify network issues based on a variety of tools / methods (e.g. packet captures, specific device (firewalls) connection logging, Cisco CMC, Cisco FMC, monitoring tools, NAC, 802.1x, & ASDM)
- Network security – evaluate current Network Security confirmation and leverage understanding of firewall, Cisco ASA, VPN, IPSec, Routers, Fire Powe FMC, Switches, proxy technologies concepts to suggest perimeter security concepts to Code 104 for implementation (e.g. DMZ, multi-tier security zones, et
- Design and recommend improvements to the operation and maintenance of the Network Admission Control (NAC) system for use on WLAN and Virtua Private Networking (VPN) access.
- Evaluate new wireless network hardware
- Install and support Cisco routers, core switches, Layer 2 and 3 switches, Wireless APs/sensors, VPN and firewalls (Cisco ASA series).
- Audit network access in order to comply with current DoD audit security requirements "Defense In Depth".
- Design and configure data center LAN technologies such as Spanning Tree, EIGRP and multi-VRF solutions.
- Utilize security technologies, specifically, Bluecoat Web Content Filter Proxies, Bluecoat Reporter, and Active Directory to harden NSWCPD systems.
- Maintain accurate documentation for the installation, maintenance and configuration activities.

3.1.2 Contractor shall provide 24 by 7 emergency Network Operations support during high priority testing or processing periods (on an as needed basis). The 24 by 7 coverage will be scheduled with the contractor when testing or processing is planned and a network outage or server down time lasting until the next business day would impact the desired testing or processing schedule. The Government Technical Point of Contact (TPOC) will request the 24 by 7 coverage a minimum of two days in advance of the required coverage. The Government will authorize overtime for this support. The Government estimates no more than 8 weeks' total required emergency coverage. Contractor shall:

- Develop test plans for wireless LAN Controller, lightweight and autonomous wireless access points (CDRL)

- Test and certify wireless network hardware, operating system versions and configurations

- Perform installation of security patches, remediation of vulnerabilities and reporting of patch compliance; advise on security patch management and remediation actions

- Apply secure configurations such as DISA Secure Technical Implementation Guidance (STIG), including the documentation and retention of objective quality evidence of the applied configuration

3.2 Task Area 2: Engineering

3.2.1 The contractor shall provide engineering services to support the overall network architecture and data, voice, and video applications operating on the network. Engineering services to include: review and analysis of application requirements; engineering planning and design assistance; equipment and component recommendation, and screening for standards compliance; installation and testing support to include verification and validation; documentation preparation /review/analysis; engineering-level monitoring of the network which includes such things as determining cause of slowed network traffic, predicting bottlenecks in advance, resolving address conflicts, improve design to virtual LAN architecture to ensure performance and enforce Government provided security controls.

3.2.2 The contractor shall provide demonstrated understanding and application of systems engineering and configuration management principals and process, mission planning/scheduling along with experience in systems engineering and sustainment of existing baseline, effectively conduct face-to-face interaction with customers and other contractors to respond to requests for information, support to technical meetings, technical interchanges and enterprise working groups. The contractor shall work independently and represent the program at meetings and working groups with Government and associate contractors. The contractor will support customer needs and support the customer in developing them into Business/Technical Requirements and establishing scope and schedule parameters to execute projects.

3.2.3 Design and installation of network extensions and cabling to support continued space conversions, including materials for NSWCPD buildings including 4, 1000, 29, 77L/H, 87, etc.

3.2.4 Server/Desktop Administration – UNIX/Linux Administration and Zone D Cybersecurity Compliance. Tasks include the installation; configuration; integration; user-registration; execution of file backups; troubleshooting and problem resolution for all Linux Systems.

3.2.5 Support architecture, design, development, utilization, authorization, maintenance of, and migration to Department of Navy authorized cloud system providers where approved by management.

3.2.6 Gather requirements via a formalized approach for requirements (i.e., Cloud, collaborations tools, DevOps, network connectivity, high performance computing, etc.)

3.2.7 Identify Department of Navy authorized offerings (NR&DE Cloud, DISA, Cloud, etc.)

3.2.8 Develop solutions to leverage authorized offerings regarding cloud technologies

3.2.9 Research possible solutions to virtualize traditionally isolated operating systems while implementing micro-segmentation for network security

3.2.10 Provide recommended solutions to gaps between existing capabilities and departmental requirements.

3.2.11 Establish POA&M addressing short, mid and long term solutions

3.2.12 Develop Change Management, provisioning, and management processes and associated documentation

3.2.13 Identify success criteria regarding cloud deployments

3.2.14 Determine cloud best fits for existing products, and a roadmap to move those projects to cloud deployment over a number of years

3.2.15 Work closely with network Infrastructure and RMF accreditation teams to overcome roadblocks to cloud deployment.

3.2.16 Align cloud deployments to DoD/DON IT security and infrastructure requirements

3.3 Task Area 3: Design/Installation of Network Extensions and Enhancements Services

3.3.1 The contractor shall design, install, test, and validate both network extensions and

modifications. The design shall include installation drawings that show the proposed cable and equipment closet. The design shall include locations and list of materials required to complete the task. Upon approval, the contractor will provide materials and schedule technicians to perform work within agreed upon time frame. The design shall be compatible with the electrical, physical, and environmental limitations of the site. The contract shall be aware of red/black separation requirements for mixed classification environments, such as TEMPEST. The contractor shall conduct validation testing and review installer test

reports after the installation of a network extension to determine compliance with the design/contract specifications and report any discrepancy to the technical point of contact (TPOC) for further action.

3.4 Task Area 4: Telecommunications Services

3.4.1 The contractor shall provide engineering services for obtaining and troubleshooting various capacity leased lines and associated equipment such as cellular repeating devices, line monitors, smart jacks, and ISDN components. The contractor shall assist in provisioning new service: submitting Requests for Service (RFS), Telecommunications Service Requests (TSR's) and research Delayed Service Reports (DSR's) when necessary. Collect, develop, and document new long-haul requirements. Ensure all circuit information is current and no inadvertent interruption of service occurs. Prepare circuit diagrams, update service agreements, and keep long-haul management folders on file for inspections and for troubleshooting purposes. Coordinate discontinued action on circuits no longer required by the Government. Maintain inventory of circuits.

3.5 Task Area 5: Server/Desktop Administration

3.5.1 The contractor shall provide the necessary labor to provide RDT&E and NMCI server/desktop administration for approximately 75 servers and Desktop Support for approximately 2500 workstations at the Philadelphia Division. Server/Desktop system administration shall include the following:

3.5.2 Provide installation, configuration, troubleshooting, patching, and problem resolution for client workstations.

3.5.3 Provide installation, configuration, troubleshooting, problem resolution and backups of VMware virtual infrastructure; tasks include:

3.5.3.1 Configuration of VMware components for connectivity and use;

3.5.3.2 Perform in-depth troubleshooting and problem analysis on a daily basis with all action steps documented each time in a trouble ticket system;

3.5.3.3 Provide patch and update management services;

3.5.3.4 Support the evolution of current architecture and processes to enable rapid, affordable, secure delivery and lifecycle support of IT products and s that meet the operational needs;

3.5.3.5 Maintain responsibility for Storage Area Networks (SAN) consolidation and optimization efforts;

3.5.3.6 Support configuration change documentation and control processes and maintaining DOD STIG Compliance.

3.5.4 Providing installation, configuration, integration, user registration, file backups,troubleshooting and problem resolution for servers associated with network operations infrastructure servers, and corporate applications.

3.5.5 Providing installation, configuration, integration, file backups, troubleshooting and problem resolution for Storage Area Networks.

3.5.6 Providing installation, configuration, integration, user registration, file backups, security patches, troubleshooting and problem resolution for collaborate environment, i.e, SharePoint, Plexus, Team Environment, and/or Lotus Notes.

3.5.7 Administration, configuration, backup and restore and problem resolution for database servers.

3.5.8 Installation of security patches on servers, remediation of vulnerabilities and reporting of patch compliance. Advise on security patches and remediation. Tasks include:

3.5.8.1 Patch vulnerabilities within the environment to ensure information is safeguarded against unauthorized access or tampering.

3.5.8.2 Ensure application of security patches for commercial products integrated into system design meet the timelines dictated by the management auth for the intended operational environment.

3.5.8.3 Integrate automated capabilities for updating or patching system software where practical, and develop processes and procedures for manual syste software updating and patching using current and projected patch timeline requirements for the system's operational environment.

3.5.8.4 Determine and document critical numbers of software patches or the extent of releases that would leave software vulnerable.

3.5.8.5 Operate and maintain the Assured Compliance Assessment Solution (ACAS)

3.5.8.6 Provide system administration and maintain operations of Nessus and Security Center.

3.5.8.7 Maintain system patches, O/S, Database, and Application STIG compliance

3.5.8.8 Update ACAS plugin Libraries, in accordance with Dept. of Navy requirements

3.5.8.9 Resolve Security Center web interface issues and Nessus network scanning issues

3.5.8.10 Configure and manage ACAS application level for user permissions, policies, scan zones, and repositories

3.5.9 Assisting the Government in managing life cycle requirements.

3.5.10 Performing routine audits of systems and software, adding, removing, or updating user accounts information, resetting passwords.

3.5.11 Answering technical queries, maintaining security posture, monitor system security, documenting system configuration, and conduct performance tuning.

3.5.12 Supporting servers and Windows Active Directory domain for PKI authentication. Support use of alternate authentication procedures for administrative access to servers.

3.5.13 Supporting configuration change documentation and control processes

3.5.14 Apply secure configurations (e.g. DISA Secure Technical Implementation Guidance (STIG)), including the documentation and retention of objective quality evidence of the applied configuration

3.5.15 Analyze event logs on all servers and apply corrective actions when necessary to ensure all servers are operational

3.5.16 Perform routine audits of server systems; adding, removing, or updating user accounts information; resetting passwords

3.5.17 Troubleshoot user problems to determine whether they are hardware, software, procedural, or communication related and provide timely resolution

3.5.18 Log and track service desk tickets using NSWCCD Philadelphia Help Desk software; maintain historical records and related problem documentation

3.5.18.1 Address all assigned service desk tickets in a timely and efficient manner

3.5.18.2 Document instances of server equipment or component failure, repair, installation, and removal using NSWCCD Philadelphia Help D

3.5.19 Monitor server systems on a daily basis to find and correct problems with disk usage, hardware, and software

3.5.20 Liaise with third-party support and server equipment vendors to resolve outstanding server issues

3.5.21 Upgrade server hardware, including memory, hard drives, external media devices (optical and non-optical), monitors, motherboards, processors, video cards, network cards, and other special purpose cards

3.6 Task Area 6: Information Management (IM), User Support

3.6.1 The contractor shall provide customer support Help Desk for all network users in Philadelphia, PA and 100+ users in remote sites. Help Desk support to remote sites will be by telephone/VTC only; Help Desk will not provide on-site customer support for the remote sites.

1. Norfolk, VA

2. San Diego, CA

3. Washington, DC

User support will include both telephone and desk side support for the Philadelphia site and will be provided from 0600 to 1800 Monday through Friday.

Help Desk services shall include the following:

3.6.2 Provide first-level usage support for locally developed applications deployed within NSWC Philadelphia Division.

3.6.3 Design, plan, implement, and use database management software to add, delete, and update user information.

3.6.4 Provide guidance to the Division’s scientific and engineering community which utilizes the provided networking, security, and other system services.

3.6.5 Troubleshoot user problems to determine whether they are hardware, software, procedural, or communication related and routing the problem to the correct support party for resolution.

3.6.6 Monitor Division-wide systems on a daily basis to find and correct problems with disk usage, hardware, and software. Post outage/maintenance updates to users through email or Intranet Web pages.

3.6.7 Produce reports from Help Desk database software for management (CDRL).

3.6.8 Track usage and problem history through Help Desk software.

3.6.9 Install devices on the network including activating the network port, configuring the device on the network, installing standard software configurations, and updating databases with device information.

3.6.10 On-site Help Desk staffing required during Philadelphia Division business hours from 0600 to 1800 EST. User support will include both telephone and desk side support for the Philadelphia site; and telephone and VTC support (but no desk side support) for the detachments/off-site users. Support will be provided from 0600 to 1800 EST Monday through Friday.

3.6.11 Manage Information Technology Procurement Requests (ITPRs) submitted into the Navy Information Technology Approval System (NAVITAS). Must have knowledge of the latest NAVADMIN policies and coordinate with other NAVITAS approvers at the Echelon II and local level to make sure all requests are moving through the workflow in a timely manner. Tasks include:

3.6.11.1 Supporting command users in the completion and proper acquisition of IT purchase approval authority through the NAVITAS system

3.6.11.2 Coordination with reviewers within and external to the Command to expedite purchase approvals or resolve concerns

3.6.11.3 Provide data entry as necessary to input necessary information within NAVITAS

3.6.11.4 Track and monitor all outstanding NAVITAS ITPRs by fiscal year

3.6.11.5 Report key performance metrics of NAVITAS ITPRs

3.7 Task Area 7: Video Telecommunications (VTC) / Audio Visual (AV)

3.7.1 The contractor shall provide support for: Video Teleconferencing (VTC) Operations, Conference Room Support, and Audio/Visual (AV) Support, Public Address (PA) System Support, and Digital Signage/Announcement Board Support at the Philadelphia sites. VTC/AV services shall include the following:

3.7.2 Provide VTC Daily Operations, set up the equipment and the VTC bridge for VTC sessions, establish the connection to the remote site or sites, operate the VTC/AV equipment (includes monitors, speakers, cameras, and microphones), ensure the AV system functions in accordance with Department of Navy requirements and customer expectations, and monitor meetings to completion.

3.7.3 Support for digital Divisional signage including updates to signage messages

3.7.4 Set up and tear down equipment in the conference rooms; portable audio system, arrange tables, chairs, easels, etc. to meet the user's requirements.

3.7.5 Support installation and configuration of new VTC, A/V, and PA hardware and the reconfiguration of existing hardware. Equipment may be added to the existing VTC or A/V configuration; therefore, the contractor shall be responsible for installing and configuring this new hardware. The contractor shall be responsible for making configurations changes (new ISDN numbers, additions to the speed dial menu or VCR recording settings, etc.).

3.7.6 Provide maintenance, troubleshooting and repair services for the VTC, A/V and conference room systems. The contractor shall troubleshoot problems with the equipment including connection issues, usage of peripheral equipment associated with each system, and audio or visual problems. Interface with the hardware maintenance provider to resolve any equipment malfunctions and provide status to Government COR.

3.7.7 Respond to requests for support of ongoing VTCs and conferences, such as changes of VTC and A/V equipment, room configurations, and similar requests.

3.7.8 Perform a variety of technical and administrative support duties to include maintaining a current inventory of all VTC, A/V, and conference room equipment (make, model, serial number, software version, account names, and passwords); assisting with general office administration duties that are associated with the operation of a conference support group (i.e. - answering the telephone, photocopying, faxing, emails, room & bridge scheduling, maintaining VTC, A/V and conference room supplies); providing support to conference attendees in the form of photocopying, media transfers and other clerical requirements.

3.7.9 Hours of VTC/AV support are from 0600 – 1800 local time. On occasion, special events may have extended hours or run during a weekend. The Government will schedule these events at least two days in advance (if possible) and approve overtime for these events.

3.8 Task Area 8: Continuity of Operations Plan (COOP)

3.8.1 The contractor will provide support of the Philadelphia Division's COOP. Tasks to be performed shall include the following:

3.8.2 Develop, implement and maintain administrative documentation, access control, inventories, communications, and Standard Operating Procedures (SOPs).

3.8.3 Develop, implement and maintain procedures for Periodic Functional Assurance Tests. Perform scheduled testing of equipment and have equipment repaired as needed.

3.8.4 Develop, implement and maintain procedures for deployment of equipment per the Division's requirements. On an established schedule, deploy

equipment and test equipment in designated areas. Deployed equipment will include NMCI/NGEN and RDT&E standard and classified seats.

3.8.5 Ensure that COOP NMCI/NGEN and RDT&E workstations are current with patches and software updates for COOP events.

3.8.6 Contractor support during non-business hours may be required during COOP trials and actual events. The Government will schedule these events at least two days in advance (if possible) and approve overtime for these events.

3.9 Task Area 9: High Performance Computing

3.9.1 The contractor shall provide computational and user support for Division Modeling and Simulation Computers. Computer support shall include maintenance of classified and unclassified systems, installation of patches, maintenance and backup of Storage Array Networks (SANs), maintenance of user accounts and audit logs. Support shall also include installation of computational software and maintenance of workstations that access computational software.

3.10 Task Area 10: Operations and Production Control

3.10.1 The contractor shall provide computer operations services in support of business data processing and the Navy's Enterprise Resource Planning (ERP) system. Computer operations services include system monitoring, troubleshooting, and processing required to update files. Computer operations requires that the functions be coordinated among and between different computer systems and jobs be submitted in the correct sequence and that processing be monitored to ensure all runs are processed correctly. Business data processing requirements at Philadelphia Division are subject to a great deal of fluctuations as new system capabilities are added and as the Division's information requirements change. Currently, the major data processing requirements are related to locally developed NMCI applications and the locally developed Corporate Database.

3.11 Task Area 11: Documentation of Network Infrastructure

3.12.1 The contractor shall research, document and create Technical drawings for the RDT&E network cabling at site. Building drawings shall be Government Furnished Information with network cable plant added as a layer to these drawings.

3.12 Task Area 12: NMCI/NGEN Support

3.12.1 The contractor shall provide labor and material to support NMCI/NGEN administration at NSWC Philadelphia Division. Support shall include the following:

3.12.2 Tracking the progress of each Move/Add/Change (MAC) request to its completion, process all NMCI account related requests, and provide direct support to the NGEN Activity Customer Technical Representative (ACTR). Liaison with the NGEN Service Request Management (SRM) Team to seek and receive from the NGEN SRM Team any new processes relating to NGEN service related MACs.

3.12.3 Customer support on contract line (CLIN) options, submitting Move/Add/Changes, ordering policies, and general NMCI/NGEN policies.

3.12.4 Perform data entry into Navy standard and local unique systems.

3.12.5 Generate reports for management analysis.

3.12.6 Gather metrics for status reporting.

3.12.7 Maintain NSWC Philadelphia Division user information to ensure NMCI/NGEN orders reflect current user data such as name, organizational code, physical location and gathering data where required.

3.12.8 Track problem reporting and resolution.

3.12.9 Coordinate NMCI/NGEN service delivery to remote site locations.

3.12.10 Gather and maintain NMCI/NGEN documentation and signed agreements.

3.12.11 Update data resident on local NMCI/NGEN web site.

3.12.12 Support integration of Government mobile devices (i.e. smartphones, cell phones, Wi-Fi cards, cellular modems) into the NMCI network. Tasks include:

3.12.12.1 Developing and maintaining an accurate inventory of all cellular devices

3.12.12.2 Tracking, issuing, and assigning cellular devices to authorized users

3.12.12.3 Maintaining and implementing workflows supporting the lifecycle of mobile devices and users

3.12.12.4 Maintaining records of signed agreements and plant property forms

3.12.12.5 Troubleshoot user problems to determine whether they are hardware, software, procedural, or communication related and provide timely resolu

3.12.12.6 Address all assigned service desk tickets in a timely and efficient manner

3.12.12.7 Liaise with third-party support and server equipment vendors to resolve outstanding server issues

3.12.13 Perform NMCI MACs - Seat Moves, Seat conversions NNPI, Peripheral Moves, Functional Mailbox creation, Functional Account creations, Distribution List creations and updates. This may include documentation supporting the relocation of equipment as well as the physical relocation of equipment.

3.12.14 Perform Account Processing - NMCI Account Creation (NIPR, SIPR, DEV, NNPI), NMCI Account Deactivation, (NIPR, SIPR, DEV, NNPI), NMCI Account transfers, SAAR processing.

3.12.15 Perform NET Corrections - Update NET records, edit / update user profiles Perform Global Address List (GAL) Updates.

3.12.16 Perform eMarketplace Task Order MODs - Work with NAVSEA and Comptroller to process and track NMCI Task orders modifications.

3.13 Task Area 13: Departmental NMCI Coordination and Support:

3.13.1 The contractor shall provide the necessary labor and materials to coordinate with and support the NSWC Philadelphia Division Activity Customer Technical Representative (ACTR) in implementing the NMCI/NGEN contract, and to act as the interface between the NMCI ACTRs and the individual users at NSWC Philadelphia Division. Contractor shall:

3.13.2 Act as the advocate for the users, troubleshooting issues as they arise with the ACTRs; interface with customers, users, and subject matter experts for NMCI/NGEN Enterprise Network specific issues; provide first-call resolution for IT service requests within the scope of NMCI/NGEN Enterprise Network

3.13.3 Forward out routine NMCI info from the ACTRs to the division, and is responsible for answering NMCI data calls requiring division level input.

3.13.4 Coordinate the division's seat orders and renewal and forwards divisional contract mods (requests for new CLINs) to the ACTRs.

3.13.5 Monitor and control custodianship and location of all NMCI/NGEN assets for the division.

3.13.6 Ensure all custodianship and location changes are achieved via the MAC process.

3.13.7 Attend monthly NMCI Seat Rep Global Issues meetings.

3.13.8 Address other NMCI issues as they arise.

3.13.9 Provide support, maintenance, operation and troubleshooting for all NMCI/NGEN Xerox Multi-functional devices (MFD) at NSWC Philadelphia. Tasks include:

3.13.9.1 Interfacing with customers, users, and subject matter experts for printer and multi-function device (MFD) specific issues

3.13.9.2 MFD account and asset management and tracking

3.13.9.3 Providing first call resolution for IT service requests regarding printers and MFDs

3.13.9.4 Managing tickets in the assigned ticket management tool, including detailed notes, time tracking, and proper attribution

3.13.9.5 Perform printer and MFD resupply as necessary including toner, drum, imager, and paper restocking

3.13.10 Tracking

3.13.10.1 Manage and account for NMCI/NGEN Enterprise Network accounts and assets;

3.13.10.2 Manage tickets in the assigned ticket management tool, including detailed notes, time tracking, and proper attribution;

3.13.10.3 Escalate and route trouble tickets to appropriate subject matter experts with supporting troubleshooting results (showing a clear description of the reported issue(s))

3.13.11 Seat Representative duties

3.13.11.1 Serve as a single point of contact for all NMCI tasks, issues, challenges, or activities within assigned department.

3.13.11.2 Process and handle Move/Reassign (MAC) requests in the Service Request Management (SRM) system. Coordinate group MACs within the as technical department and provide guidance to customers regarding the MAC process, including timelines associated with specific requests.

3.13.11.3 Coordinate NMCI support activities with the Technical Department Head and associated Department Head Administrative Officers (AOs); acti an advocate for customers when troubleshooting NMCI issues and provide desktop support for customers with NMCI issues. (For issues beyond the Seat capabilities, the customer must possess an open NMCI Helpdesk Ticket to resolve the issue by calling the national number 866-843-6624 24-hour servic assistance. NMCI Seat Reps will assist, as necessary.

3.13.11.4 Maintain access to NMCI Enterprise Tool (NET) to administer necessary changes and updates.

3.13.11.5 Coordinate the distribution and delivery of new NMCI hardware to customers within assigned departments.

3.13.11.6 Use the Service Request Management (SRM) system to update accurately with new or changed NMCI assets and customer information (e.g. ne customer assignments, seat moves).

3.13.11.7 Provide respective workforce within the technical departments with information on available current NMCI services and inform management o NMCI issues, updates and other pertinent information (provided by NMCI team) regarding NMCI workstations & NMCI accounts.

3.13.11.8 Coordinate technical refresh seat orders; collect and remove old NMCI equipment in accordance with guidance provided by the Code 104 NM team, which consists of the Activity Contract Technical Representatives (ACTRS) and Code 1042 Branch Head.

3.13.11.9 Deliver hands on assistance to customers with the initial setup of all NMCI equipment, mobile devices and ensure ongoing maintenance.

3.13.11.10 Track the status of NMCI tickets and initiate corrective actions daily.

3.14 Task Area 14: Administrative and graphics Support for NSWCPD Code 104

3.14.1 Contractor shall provide financial analysis and management and preparation of presentation materials. Contractor shall provide on-site administrative services and support assistance as directed including word processing, copy and file letters, reports, memos, travel orders, travel vouchers, and other similar types of documents. Maintain currency of correspondence procedures in accordance with our local instructions. All correspondence shall be proofread, edited, and corrected for errors in format and grammar. Contractor shall maintain master project calendar and coordinating arrangements for presentation/meetings.; record time and attendance using ERP; entering purchase requests into ERP (excluding contracts PRs and PRs specifically for the Contractor); help support network account information on System Access Authorization Request (SAAR) forms.

3.14.2 Also enter data into various computerized databases and tracking systems and create spreadsheets and graphs based on the information contained in these systems; and manage office supplies. Maintain hard copies of direction, instructions, and other documents that are required to support documentation audits.

3.14.3 Contractor shall assist with NSWC Philadelphia Division security badge information entry and security badge documentation processing. Contractor shall provide on-site administration services to process and track badge and swipe card services and support assistance requests in accordance with our Division instructions and procedures.

3.14.4 The Contractor shall be familiar with the design and development of graphic/visual effects used in presentations, meetings and reports. The contractor shall be responsible for the use of specialized computer software to develop high quality computer illustrations, technical drawings, and/or animations to support various media. The Contractor is capable of using specialized hardware and/or software for video/audio capture and editing of multimedia presentations, incorporates principles of layout design throughout the production process, and is responsible for quality control, review and revision of all aspects of graphics development.

3.14.5 The contractor shall be responsible for Administration/maintenance of the IT Asset Management and Help Desk Workflow system supporting the RDT&E environment and oversight of all ‘on the shelf’ hardware and software inventories in support of RDT&E IT Operations. Tasks include:

3.14.5. 1 The design, development, and implementation of an IT asset management process and workflow across the enterprise

3.14.5.2 Ensuring FISMA compliance with IT asset management guidelines as well as ensuring that only National Information Assurance Partnership (N compliant computer hardware and software are implemented, inventoried, and maintained by the organization.

3.14.5.3 Ensuring end-to-end integration of the IT asset procurement, maintenance, and disposal processes to be in compliance with FISMA, DOD, and I cyber security policies and directives; ensuring only NIAP compliant hardware and software are implemented and maintained; coordination of inventory alignment activities with Command Plant Property managers.

3.14.5.4 Administration/maintenance of IT Asset Management and Help Desk Workflow system supporting the RDT&E environment and oversight of all the shelf’ hardware and software inventories in support of RDT&E IT Operations

3.14.5.5 Administer data integration and sharing with Philadelphia document management system.

3.15 Task Area 15: Cybersecurity

3.15.1 The contractor shall provide the necessary labor to support Cybersecurity efforts for approximately 2,500 assets (desktops, laptops, and servers). Cybersecurity efforts shall include:

3.15.2 Vulnerability Assessment of Windows and Linux/UNIX systems including:

3.15.2.1 Vulnerability Scanning & Identification

3.15.2.2 Secure Configuration (e.g. STIG (Security Technical Implementation Guides))

3.15.2.3 Implementation and Verification

3.15.2.4 The remediation and mitigation of identified deficiencies through research and the application of suggested remediation or mitigation

3.15.2.5 Planning of the deployment and installation of HBSS servers

3.15.3 Endpoint Compliance including:

3.15.3.1 Host Based Security products, their management, and deployment

3.15.3.2 Antivirus management including updates, executing scans, and interpreting results

3.15.3.3 Automated software and patch distribution

3.15.3.4 Standard endpoint imaging processes

3.15.3.5 Implement HBSS migration/compliance strategy.

3.15.3.6 Troubleshoot HBSS product issues and outages.

3.15.3.7 Administer McAfee ePolicy Orchestrator (ePO) tree structure management.

3.15.3.8 Maintain system patches, O/S, SQL, and HBSS STIG compliance.

3.15.3.9 Resolve ePO server (O/S, ePO, or SQL) issues.

3.15.3.10 Maintain the ePO server (automated tasks, task scheduler, database maintenance tasks, etc.).

3.15.4 Knowledge of assessment and authorization (A&A) practices in accordance with the Department of Defense Risk Management Framework (RMF), in accordance with the current published Department of Navy RMF Process Guide, including:

3.15.4.1 Proper documentation of residual risks in a plan of actions and milestones formatted in compliance with the current package system, currently eMASS

3.15.4.2 Tracking of deliverables and action items in accordance with A&A guidance

3.15.4.3 Knowledge of existing DON and DoD policies to ensure package compliance with stated Policy

3.15.4.4 Manage, attend, and support configuration control board practices

3.15.4.5 Maintain current vulnerability scan data and residual risk plan of actions and milestones in Vulnerability Remediation Asset Manager (VRAM)

3.15.4.6 Perform risk management and security engineering for Zone D boundaries to include IAVM support, remediation, patching, scanning and associated boundary maintenance

3.15.5 Intrusion Detection and Prevention including:

3.15.5.1 Network perimeter ID/PS monitoring, adjudication, and reporting to the chain of command

3.15.5.2 Host based ID/PS monitoring, adjudication, and reporting to the chain of command

3.16 Task Area 16: Information Technology Support/Coordination (ITC)

3.16.1 The contractor shall provide the necessary labor to coordinate all Departmental Information Technology/Cybersecurity issues. Information Technology

Support/Coordination will be required to understand a Department's technical capabilities and mission work to ensure accurate impact assessments are performed. The contractor shall ensure integration with IA/IT to leverage Division wide lessons learned for the efficient delivery of technical solutions and issue resolution.

3.17 Task Area 17: Data Base Administration

3.17.1 Coordinate changes to computer databases, test and implement the database applying knowledge of database management systems. Plan, coordinate, and implement security measures to safeguard computer databases.

3.17.2 Modify existing databases and database management systems or note actions required of programmers and analysts to implement the changes.

3.17.3 Test programs or databases, correct errors and make necessary modifications.

3.17.4 Plan, coordinate and implement security measures to safeguard information in computer files against accidental or unauthorized damage, modification or disclosure.

3.17.5 Schedule, plan, and execute the installation and testing of new products and improvements to computer systems, such as the installation of new databases.

3.17.6 Establish and calculate optimum values for database parameters, using manuals and calculator.

3.17.7 Specify users and user access levels for each segment of database.

3.17.8 Develop data model describing data elements and how they are used, following procedures and using pen, template or computer software.

3.17.9 Develop methods for integrating different products so they work properly together, such as customizing commercial databases to fit specific needs.

3.17.10 Review project requests describing database user needs to estimate time and cost required to accomplish project.

3.17.11 Review procedures in database management system manuals for making changes to database.

3.17.12 Work as part of a project team to coordinate database development and determine project scope and limitations.

3.17.13 Select and enter codes to monitor database performance and to create production database.

3.17.14 Identify and evaluate industry trends in database systems to serve as a source of information and advice for upper management.

3.17.15 Write and code logical and physical database descriptions and specify identifiers of database to management system or direct others in coding descriptions.

3.17.16 Review workflow charts developed by programmer analyst to understand tasks computer will perform, such as updating records.

3.17.17 Analyze and plan for anticipated changes in data capacity requirements.

3.17.18 Review and validate data mining and data warehousing programs, processes, and requirements.

3.17.19 Develop data standards, policies, and procedures for Government review.

3.17.20 Maintain directory replication services that enable information to replicate automatically from rear servers to forward units via optimized routing.

3.17.21 Maintain information exchanges through publish, subscribe, and alert functions that enable users to send and receive critical information as required.

3.17.22 Manage the compilation, cataloging, caching, distribution, and retrieval of data.

3.17.23 Monitor and maintain databases to ensure optimal performance.

3.17.24 Perform backup and recovery of databases to ensure data integrity

3.17.25 Performs configuration management, problem management, capacity management, and financial management for databases and data management systems.

3.17.26 Participate in the Risk Management Framework authorization process

3.17.27 Perform integrated quality assurance testing for security functionality and resiliency attacks.

3.17.28 Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.

3.18 Task Area 18: Software Development

3.18.1 The contractor shall provide ongoing operation, maintenance, troubleshooting and diagnostics, development and administration support for Philadelphia Division Intranet (PDI)- SharePoint, myPD and iNAVSEA database programming including Oracle and SQL programming. Tasks include:

3.18.1 Analysis of users' needs and for the design, construct, test, and maintenance of computer applications software and systems.

3.18.2 Design and development of various types of software, including software for operating systems and network distribution, and compilers, which co programs for execution on a computer.

3.18.3 Execute tasks in accordance with a principled systems engineering process such as CMMI.

4.0 DATA REQUIREMENTS

4.1 Contract Status Report (**CDRL A001**)

4.2 Travel Report (**CDRL A002**)

4.3 Contractor's Personnel Roster (**CDRL A003**)

4.4 Cyber Security Workforce (CSWF) Baseline Certifications (**CDRL A004**)

4.5 Cybersecurity Workforce (CSWF) Computing Environment /Operating System (CE/OS) Certifications (**CDRLA005**)

4.6 These reports shall reflect both prime and Subcontractor data if applicable and at the same level of detail. The CDRLs shall be delivered electronically unless otherwise stated, and while Contractor's format is acceptable, Government's approval is required from the COR.

5.0 SECURITY REQUIREMENTS

5.1 An Active (SECRET) Facility Clearance (FCL) is required for performance on this contract. There are no safeguarding requirements required.

5.1.1 The resultant contract involves classified information or material associated with classified information. All contractor personnel working on this resultant contract and performing its required services on site, as reflected in Item 8 of the DD254, shall be United States citizens only, information is not releasable to foreign national, and shall possess and maintain at a minimum at the SECRET level. Interim clearances are acceptable. No classified data will be generated or stored by the Contractor. The requirements of the attached DD Form 254 apply.

5.1.2 The Contractor is responsible for completing all required Government mandated training to maintain security and network access to Government sites and IT systems to include but not limited to:

- Antiterrorism Level 1 Awareness;
- DoD Cyber Awareness Challenge;
- Combatting Human Trafficking;
- Records Management in the DON: Everyone's Responsibility;
- Training and Readiness:
- The Active Shooter;
- Constitution Day;
- NAVSEA Introduction to Controlled Unclassified Information;
- Operations Security (OPSEC);
- NAVSEA Counterintelligence Training;
- Privacy and Personally Identifiable Information (PII) Awareness Training;
- NAVSEA Physical Security training.

Certificates of successful completion shall be sent to the COR and as otherwise specified in the contract.

5.2 Naval Nuclear Propulsion Information (NNPI)

Security Classification Guidance follows portions of the tasking on this contract when invoked in the task order statement of work:

5.2.1 Contractor requires access to information and equipment classified at the (Secret) National Security Information (NSI) level in order to provide industrial support services within facilities that actively supports the Navy Nuclear Propulsion Program (NNPP).

5.2.2 The resultant contract involves classified information or material associated with classified information. All contractor personnel working on this resultant contract must be United States citizens, no foreign nationals, and shall have and maintain at a minimum (Secret) security clearance. Interim clearances are acceptable.

5.2.3 The Contractor is responsible for completing all required Government mandated training to maintain security and network access to Government sites and IT systems, as necessary to support.

5.3 Unclassified Naval Nuclear Propulsion Information (U-NNPI)

5.3.1 Purpose.

The contractor hereby agrees that when provided documents (specifications, drawings, etc.) that are marked as containing NOFORN sensitive information that must be controlled pursuant to Federal law, the information contained therein and generated as part of the inquiry shall be used only for the purpose stated in the contract and shall in no case be transmitted outside the company (unless such transmittals comply with the detailed guidance of the contract) or to any foreign national within the company. While in use, the documents shall be protected from unauthorized observation and shall be kept secure so as to preclude access by anyone not having a legitimate need to view them. The documents shall not be copied unless done in conformance with the detailed guidance of the contract. All the documents shall be promptly returned in their entirety, unless authorized for proper disposal or retention, following completion of the contract.

5.3.2 Specific Requirements for Protecting U-NNPI

a) Only U.S. citizens who have an NTK required to execute the contract shall be allowed access to U-NNPI.

b) When not in direct control of an authorized individual, U-NNPI must be secured in a locked container (e.g., file cabinet, desk, safe). Access to the container must be such that only authorized persons can access it, and compromise of the container would be obvious at sight. Containers should have no labels that indicate the contents. If removed from the site, U-NNPI must remain in the personal possession of the individual. At no time should U-NNPI be left unsecured (e.g., in a home or automobile, or unattended in a motel room or sent with baggage).

c) U-NNPI documents will have the word NOFORN at the top and bottom of each page. Documents originated in the course of work that reproduce, expand or modify marked information shall be marked and controlled in the same way as the original. Media such as video tapes, disks, etc., must be marked and controlled similar to the markings on the original information.

d) U-NNPI may not be processed on networked computers with outside access unless approved by CNO (N00N). If desired, the company may submit a proposal for processing NNPI on company computer systems. Personally owned computing systems, such as personal computers, laptops, personal digital assistants, and other portable electronic devices are not authorized for processing NNPI. Exceptions require the specific approval of the cognizant DAA and CNO (N00N).

e) U-NNPI may be faxed within the continental United States and Hawaii provided there is an authorized individual waiting to receive the document and properly control it. U-NNPI may not be faxed to facilities outside the continental United States, including military installations, unless encrypted by means approved by CNO (N00N).

f) U-NNPI may be sent within the continental United States and Hawaii via first class mail in a single opaque envelope that has no markings indicating the nature of the contents.

g) Documents containing U-NNPI shall be disposed of as classified material.

h) Report any attempts to elicit U-NNPI by unauthorized persons to the appropriate security personnel.

i) Report any compromises of U-NNPI to the appropriate security personnel. This includes intentional or unintentional public release via such methods as theft, improper disposal (e.g., material not shredded, disks lost), placement on Web site, transmission via email, or violation of the information system containing U-NNPI.

6.0 PLACE OF PERFORMANCE

6.1 The contractor shall primarily perform work in support of this contract onsite at NSWC Philadelphia Division, Philadelphia, PA. Alternate work locations, may be utilized if deemed appropriate.

6.2 Occasional travel may be required between Philadelphia and Remote Sites located throughout the continental United States.

6.3 On-site office space shall be made available to the contractor in performance of this task order as required. Contractor personnel may also work at the

contractor's off-site location when deemed appropriate and specified by the Contracting Officer's Representative. The Government will provide each individual an NMCI workstation.

6.3.1 Government will provide office space and seating, phones, computers and make available printers and phone/network connections space for the Contractor personnel under this task order.

6.3.2 The specific location(s) will be provided at time of award of the task order. The Contractor shall provide a list of employees who require access to these areas, including standard security clearance information for each person, to the Contracting Officer Representative (COR) no later than three business days after the date of award. The work space provided to the Contractor personnel shall be identified by the Awardee, with appropriate signage listing the company name and individual Contractor employee name.

6.3.3 Access to Government buildings at Naval Surface Warfare Center Philadelphia Division is from 0600 to 1800 Monday through Friday, except Federal holidays. Normal work hours are from 0600 to 1800, Monday through Friday. Contractor employees shall be under Government oversight at all times. Government oversight requires that a Government employee be present in the same building/facility whenever Contractor employee(s) are performing work under this task order. Contractor personnel are not allowed to access any Government buildings at NSWCPD outside the hours of 0600 to 1800 without the express approval of the Procuring Contracting Officer (PCO).

6.4 Early Dismissal and Closure of Government Facilities

6.4.1 When a Government facility is closed and/or early dismissal of Federal employees is directed due to severe weather, security threat, or a facility related problem that prevents personnel from working, onsite Contractor personnel regularly assigned to work at that facility should follow the same reporting and/or departure directions given to Government personnel. The Contractor shall not direct charge to the contract for time off, but shall follow its own company policies regarding leave. Non-essential Contractor personnel, who are not required to remain at or report to the facility, shall follow their parent company policy regarding whether they should go/stay home or report to another company facility. Subsequent to an early dismissal and during periods of inclement weather, onsite Contractors should monitor radio and television announcements before departing for work to determine if the facility is closed or operating on a delayed arrival basis.

6.4.2 When Federal employees are excused from work due to a holiday or a special event (that is unrelated to severe weather, a security threat, or a facility related problem), on site Contractors will continue working established work hours or take leave in accordance with parent company policy. Those Contractors who take leave shall not direct charge the non-working hours to the task order. Contractors are responsible for predetermining and disclosing their charging practices for early dismissal, delayed openings, and closings in accordance with the FAR, applicable cost accounting standards, and company policy. Contractors shall follow their disclosed charging practices during the task order period of performance, and shall not follow any verbal directions to the contrary. The PCO will make the determination of cost allowability for time lost due to facility closure in accordance with FAR, applicable Cost Accounting Standards, and the Contractor's established accounting policy.

7.0 TRAVEL

7.1 The Contractor may be required to travel from the primary performance location when supporting this requirement. The estimated number of trips is 4 per year.

Travel in support of this requirement is anticipated to include, but may not be limited to, the following alternate performance locations:

1. Norfolk, VA

2. San Diego, CA

3. Washington, DC

The number of times the Contractor may be required to travel to each location cited above may vary as program requirements dictate, provided that the total estimated travel cost is not exceeded. The numbers of trips and types of personnel traveling shall be limited to the minimum required to accomplish work requirements. All travel shall be approved by the COR and Contracting Officer before travel occurs. Approval may be via the Technical Instruction (TI). Before initiating any travel, the Contractor(s) shall submit a detailed and fully-burdened estimate that includes the number of employees traveling, their expected travel costs for airfare, lodging, per diem, rental car, taxi/mileage and any other costs or actions requiring approval. The travel estimate shall be submitted to the Contracting Officer's Representative (COR) and Contract Specialist. Actuals cost, resulting from the performance of travel requirements, shall be reported as part of the Contractor's monthly status report. The reportable cost shall also be traceable to the Contractor's invoice

7.1.1 All travel shall be conducted in accordance with FAR 31.205-46, Travel Costs, and B-231-H001 Travel Costs (NAVSEA) (OCT 2018) and shall be pre-approved by the COR. The Contractor shall submit travel reports in accordance with DI-MGMT-81943 (CDRL A002).

7.2 Travel Costs

The current "maximum per diem" rates are set forth in the (i) Federal Travel Regulations for travel in the Continental United States; (ii) Joint Travel

Regulations for Overseas Non-Foreign areas (e.g., Alaska, Hawaii, Guam, Puerto Rico, etc.); and (ii) Department of State (DOS) prescribed rates for foreign overseas locations.

8.0 GOVERNMENT FURNISHED PROPERTY

Not Applicable

9.0 GOVERNMENT FURNISHED INFORMATION

Not Applicable

10.0 PURCHASES

10.1 Only items directly used for this Task Order, for work within the scope of the Performance Work Statement, shall be purchased under the Other Direct Cost (ODC) line items. Individual non-IT purchases above $10,000 shall be approved by the Contracting Officer prior to purchase by the Contractor. The purchase request and supporting documentation shall be submitted via email to the Contracting Officer and the Contracting Officer's Representative (COR) it shall be itemized and contain the cost or price analysis performed by the Contractor to determine the reasonableness of the pricing.

10.1.1 Information Technology (IT) equipment, or services must be approved by the proper approval authority. All IT requirements, regardless of dollar amount, submitted under this Task Order shall be submitted to the PCO for review and approval prior to purchase. The definition of information technology is identical to that of the Clinger-Cohen Act, that is, any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

11.0 COUNTERFEIT MATERIAL PREVENTION

11.1 Counterfeit End-Items

11.1.1 For purposes of this section, a "Counterfeit Item" is defined to include, but is not limited to, (i) an item that is an illegal or unauthorized copy or substitute of an OM item; (ii) an item that does not contain the proper external or internal materials or components required by the OM or that is not constructed in accordance with OM specification; (iii) an item or component thereof that is used, refurbished or reclaimed but the Seller represents as being a new item; (iv) an item that has not successfully passed all OM required testing, verification, screening and quality control but that Seller represents as having met or passed such requirements; (v) an item with a label or other marking intended, or reasonably likely, to mislead a reasonable person into believing a non-OM item is a genuine OM item when it is not or (vi) material that has been confirmed to be a copy, imitation or substitute that has been represented, identified or marked as genuine, and/or altered by a source without legal right with intent to mislead, deceive or defraud.

11.2 Software

11.2.1 Seller warrants that any hardware, software and firmware goods delivered under this Contract: (i) shall not contain any viruses, malicious code, Trojan horse, worm, time bomb, self-help code, back door, or other software code or routine designed to: (a) damage, destroy or alter any software or hardware; (b) reveal, damage, destroy, or alter any data; (c) disable any computer program automatically; or (d) permit unauthorized access to any software or hardware; (ii) shall not contain any third party software (including software that may be considered free software or open source software) that (a) may require any software to be published, accessed or otherwise made available without the consent of Buyer, or (b) may require distribution, copying or modification of any software free of charge; and (iii) shall not infringe any patent, copyright, trademark, or other proprietary right of any third party or misappropriate any trade secret of any third party.

11.3 Goods Warranty; Anti-Counterfeit Mitigation

11.3.1 Seller warrants the Goods delivered pursuant to this Contract, unless specifically stated otherwise in this Contract, shall (i) be new; (ii) be and only contain materials obtained directly from the OM or an authorized OM reseller or distributor (Note - Independent Distributors (Brokers) shall not be used by Seller without written consent from Buyer); (iii) not be or contain Counterfeit Items; (iv) contain only authentic, unaltered OM labels and other markings; (v) have documentation made available upon request that authenticates traceability to the applicable OM; and (vi) be free from defects in workmanship, materials, and design and conform to all the specifications and requirements of this Subcontract. These warranties shall survive inspection, test, final acceptance and payment of Goods and Services.

11.4 Preventing Counterfeit Parts and Materials

11.4.1 The Contractor shall take steps as defined in DFARS 252.246-7007 and herein to minimize the risk of receiving counterfeit parts and materials. The Contractor shall:

11.4.2 Maximize availability of authentic, originally designed and/or qualified parts throughout the product's life cycle, including management of parts obsolescence

11.4.3 Assess potential suppliers to minimize the risk of receiving counterfeit parts or materials

11.4.4 Maintain a listing of approved suppliers with documented criteria for approval and removal of suppliers from the list

11.4.5 Have purchasing procedures which require the selection of parts and materials from OM or authorized suppliers whenever possible

11.4.6 Require a certificate of compliance and supply chain traceability for all electronic part purchases, and provide to the Government upon request

11.4.7 Use Government or industry services such as GIDEP and other commercially available services to identify part or supplier quality or authenticity problems

11.4.8 Define minimum inspection and test requirements for parts being procured from unauthorized suppliers, and shall ensure that in-house, third-party, and/or distributor inspection and test procedures and facilities comply with these requirements

11.4.9 Incorporate procurement clauses which plainly identify quality requirements and liability to all approved suppliers

11.4.10 Flow the requirements above to affected Subcontractors

11.4.11 SAE AS6174 contains information regarding the detection, avoidance, and mitigation of counterfeit materiel, and may be used as a reference document for meeting the above steps.

11.4.12 Parts and materials shall not be purchased from unauthorized sources (e.g. independent distributor or broker).

11.5 Grey Market Statement (For CISCO Equipment)

11.5.1 Reseller and Equipment Qualification: Reseller shall certify that it is a CISCO Authorized Channel Partner as of the date of the submission of their offer, and that it has the certification/specialization level required by the Manufacturer to support both the product sale and product pricing, in accordance with the applicable Manufacturer certification/specialization requirements: Please provide proof of certification level with your quote submission. If proof of certification level is not provided with your quote submission, your quote may be considered non-responsive.

11.5.2 Vendor shall warrant that the products are NEW and in their original UNOPENED box. Only CISCO installed and configured components are acceptable. Installation and / or configuration of third party components, or installation and / or configuration of OM components by any other than CISCO are NOT acceptable. The Vendor confirms to have sourced all Manufacturer products submitted in this offer from Manufacturer or through Manufacturer Authorized Channels only.

11.5.3 Vendor shall provide Buyer with a copy of the End User license agreement pre-award, and shall certify that all Manufacturer software is licensed originally to Buyer as the original licensee authorized to use the Manufacturer Software. Only authentic OM equipment and support services sourced from authorized OM channels are acceptable. Equipment, materials, and services not meeting the above stated qualifications are not acceptable and will be returned to the reseller.

11.6 Containing Counterfeit Parts and Materials

11.6.1 Suspect counterfeit parts and materials shall be impounded with all other items from the same lot. The contractor shall identify and locate all potential users or hardware items with the suspect part or material, and contain product which has this suspect product, pending confirmation of the part or material's authenticity. The OM may be involved at this point in order to verify authenticity.

11.6.2 Confirmed counterfeit material shall be contained and provided to investigative agencies for ongoing investigation or prosecution. The counterfeit product shall not be scrapped or otherwise disposed of without approval from investigative authorities or the program office.

11.6.3 Confirmed counterfeit product shall not be returned or handled in a way which would allow its resale or reuse. Suspect counterfeit parts or materials whose authenticity (or lack of) cannot be definitively determined, shall be dispositioned via Material Review Board (MRB).

11.7 Nonconforming Material and Parts

11.7.1 Electrical components which fail during production or acceptance testing shall be assessed to determine if the supplier of the part was an authorized supplier for the manufacturer. Analysis of these failures shall include assessment of part authenticity (potential of being counterfeit or fraudulent).

11.8 Warranty “Counterfeit”

11.8.1 Seller warrants the goods delivered pursuant to this Contract, unless specifically stated otherwise in this Contract, shall (i) be new (ii) be free from defects in workmanship, materials, and design and (iii) be in accordance with all the requirements of this Contract. Seller further warrants that the performance of work and services shall conform with the requirements of this Contract and to high professional standards. All warranties in this Contract shall survive inspection, test, final acceptance and payment of goods and services.

12.0 PERSONNEL

12.1 Personnel Requirements.

12.1.1 All persons proposed in key and non-key labor categories shall be U.S. citizens holding at minimum a current SECRET clearance, or ability to obtain one. Interim clearances are acceptable.

12.1.2 Clause 52.222-2 "Payment for Overtime Premiums" will provide for the total approved dollar amount of overtime premium or will state “zero” if not approved. If overtime premium has not been approved under this contract in accordance with Clause 52.222-2, overtime effort to be performed shall be requested from the Contracting Officer prior to performance of premium overtime. For overtime premium costs to be allowable costs; the Contracting Officer is required to approve the performance of overtime prior to the actual performance of overtime. The dollar amount in FAR 52.222-2 shall equal overtime premium negotiated between the Government and the prime contractor. This overtime premium amount shall equal the prime contractor's unburdened premium OT labor costs plus the subcontractors' fully-burdened premium OT labor costs.

12.1.3 The table below includes the NSWCPD Labor Category (LCAT), eCRAFT Labor Category (LCAT), eCRAFT Code, and the number of Resumes required for key personnel for proposal:

NSWCPD Labor Category (LCAT)	eCRAFT Labor Category (LCAT)	eCRAFT Code	Resume Rqd. (Key)
Project Manager	Manager, Program/ Project II	MANPII	1
Server Administrator (Windows Admin)	Systems Administrator III	SA3	2
Virtualization Administrator	Systems Administrator III	SA3	2
Cybersecurity Technician (IAVM Patch Manager)	Systems Administrator II	SA2	0
Software Engineer (programming)	Engineer, Computer II	EC2	0
Sr. Security Network Engineer	Engineer, Systems III	ESY3	2
Jr. Security Network Engineer	Engineer, Systems II	ESY2	0
Linux Administrator	Systems Administrator III	SA3	2
Database Administrator	Systems Administrator II	SA2	1
McAfee HBSS EPO* Administrator	Specialist, Information Systems Security III	SISS3	1
Software Engineer (Database)	Engineer, Computer II	EC2	0
NMCI* Service Representative	Systems Administrator I	SA1	0
VTC* Technician	Engineer, Electrical/ Electronics II	EE2	0
Customer Support Representative	Systems Administrator II	SA2	0
NMCI Seat Representative	Specialist, Public Affairs	SPA	0
MFD technician	Manager, Administrative I	MANA1	0
Network Cable Installer	Engineer, Electrical/ Electronics II	EE2	0
Administrator Support	Manager, Administrative I	MANA1	0
Information/ Inventory Technology Specialist	Specialist, Configuration MGMT I	SCM1	0
Business Analyst (NAVITAS)	Acquisition Management Support II	AMS2	0
Cellular Support	Specialist, Configuration MGMT I	SCM1	0
Senior Data Storage Administrator (Cloud Architect)	Systems Administrator III	SA3	0

12.1.4 The level of effort for the performance of the resultant task order is based on the following labor categories and hours per year:

BASE YEAR				
NSWCPD Labor Category (LCAT)	**eCRAFT Labor Category (LCAT)**	**eCRAFT Code**	**Hours**	**OT Hrs.**
Project Manager	Manager, Program/ Project II	MANPII	1,920	0
Server Administrator (Windows Admin)	Systems Administrator III	SA3	7,680	922
Virtualization Administrator	Systems Administrator III	SA3	5,760	691
Cybersecurity Technician (IAVM Patch Manager)	Systems Administrator II	SA2	3,840	461
Software Engineer (programming)	Engineer, Computer II	EC2	5,760	0
Sr. Security Network Engineer	Engineer, Systems III	ESY3	5,760	691
Jr. Security Network Engineer	Engineer, Systems II	ESY2	5,760	691
Linux Administrator	Systems Administrator III	SA3	5,760	691
Database Administrator	Systems Administrator II	SA2	1,920	230
McAfee HBSS EPO* Administrator	Specialist, Information Systems Security III	SISS3	3,840	461
Software Engineer (Database)	Engineer, Computer II	EC2	1,920	0
NMCI* Service Representative	Systems Administrator I	SA1	7,680	0
VTC* Technician	Engineer, Electrical/ Electronics II	EE2	5,760	691
Customer Support Representative	Systems Administrator II	SA2	11,520	1,383
NMCI Seat Representative	Specialist, Public Affairs	SPA	19,200	2,304
MFD technician	Manager, Administrative I	MANA1	3,840	0
Network Cable Installer	Engineer, Electrical/ Electronics II	EE2	3,840	0
Administrator Support	Manager, Administrative I	MANA1	9,600	0
Information/ Inventory Technology Specialist	Specialist, Configuration MGMT I	SCM1	1,920	0
Business Analyst (NAVITAS)	Acquisition Management Support II	AMS2	5,760	231
Cellular Support	Specialist, Configuration MGMT I	SCM1	3,840	154
Senior Data Storage Administrator (Cloud Architect)	Systems Administrator III	SA3	1,920	0
BASE YEAR Total			124,800	9,601
OPTION YEAR 1				
NSWCPD Labor Category (LCAT)	**eCRAFT Labor Category (LCAT)**	**eCRAFT Code**	**Hours**	**OT Hours**
Project Manager	Manager, Program/ Project II	MANPII	1,920	0
Server Administrator (Windows Admin)	Systems Administrator III	SA3	7,680	922
Virtualization Administrator	Systems Administrator III	SA3	5,760	691
Cybersecurity Technician (IAVM Patch Manager)	Systems Administrator II	SA2	3,840	461
Software Engineer (programming)	Engineer, Computer II	EC2	5,760	0
Sr. Security Network Engineer	Engineer, Systems III	ESY3	5,760	691
Jr. Security Network Engineer	Engineer, Systems II	ESY2	5,760	691
Linux Administrator	Systems Administrator III	SA3	5,760	691
Database Administrator	Systems Administrator II	SA2	1,920	230
McAfee HBSS EPO* Administrator	Specialist, Information Systems Security III	SISS3	3,840	461
Software Engineer (Database)	Engineer, Computer II	EC2	1,920	0
NMCI* Service Representative	Systems Administrator I	SA1	7,680	0
VTC* Technician	Engineer, Electrical/ Electronics II	EE2	5,760	691
Customer Support Representative	Systems Administrator II	SA2	13,440	1,613
NMCI Seat Representative	Specialist, Public Affairs	SPA	21,120	2,535
MFD technician	Manager, Administrative I	MANA1	3,840	0
Network Cable Installer	Engineer, Electrical/ Electronics II	EE2	3,840	0
Administrator Support	Manager, Administrative I	MANA1	9,600	0
Information/ Inventory Technology Specialist	Specialist, Configuration MGMT I	SCM1	1,920	0
Business Analyst (NAVITAS)	Acquisition Management Support II	AMS2	5,760	231
Cellular Support	Specialist, Configuration MGMT I	SCM1	3,840	154
Senior Data Storage Administrator (Cloud Architect)	Systems Administrator III	SA3	1,920	0
OPTION YEAR 1 Total			128,640	10,062
OPTION YEAR 2				

NSWCPD Labor Category (LCAT)	eCRAFT Labor Category (LCAT)	eCRAFT Code	Hours	OT Hours
Project Manager	Manager, Program/ Project II	MANPII	1,920	0
Server Administrator (Windows Admin)	Systems Administrator III	SA3	7,680	922
Virtualization Administrator	Systems Administrator III	SA3	5,760	691
Cybersecurity Technician (IAVM Patch Manager)	Systems Administrator II	SA2	3,840	461
Software Engineer (programming)	Engineer, Computer II	EC2	5,760	0
Sr. Security Network Engineer	Engineer, Systems III	ESY3	5,760	691
Jr. Security Network Engineer	Engineer, Systems II	ESY2	5,760	691
Linux Administrator	Systems Administrator III	SA3	5,760	691
Database Administrator	Systems Administrator II	SA2	1,920	230
McAfee HBSS EPO* Administrator	Specialist, Information Systems Security III	SISS3	3,840	461
Software Engineer (Database)	Engineer, Computer II	EC2	1,920	0
NMCI* Service Representative	Systems Administrator I	SA1	7,680	0
VTC* Technician	Engineer, Electrical/ Electronics II	EE2	5,760	691
Customer Support Representative	Systems Administrator II	SA2	15,360	1,843
NMCI Seat Representative	Specialist, Public Affairs	SPA	23,040	2,765
MFD technician	Manager, Administrative I	MANA1	3,840	0
Network Cable Installer	Engineer, Electrical/ Electronics II	EE2	3,840	0
Administrator Support	Manager, Administrative I	MANA1	9,600	0
Information/ Inventory Technology Specialist	Specialist, Configuration MGMT I	SCM1	1,920	0
Business Analyst (NAVITAS)	Acquisition Management Support II	AMS2	5,760	231
Cellular Support	Specialist, Configuration MGMT I	SCM1	3,840	154
Senior Data Storage Administrator (Cloud Architect)	Systems Administrator III	SA3	1,920	0
OPTION YEAR 2 Total			132,480	10,522
OPTION YEAR 3				
NSWCPD Labor Category (LCAT)	**eCRAFT Labor Category (LCAT)**	**eCRAFT Code**	**Hours**	**OT Hours**
Project Manager	Manager, Program/ Project II	MANPII	1,920	0
Server Administrator (Windows Admin)	Systems Administrator III	SA3	7,680	922
Virtualization Administrator	Systems Administrator III	SA3	5,760	691
Cybersecurity Technician (IAVM Patch Manager)	Systems Administrator II	SA2	3,840	461
Software Engineer (programming)	Engineer, Computer II	EC2	5,760	0
Sr. Security Network Engineer	Engineer, Systems III	ESY3	5,760	691
Jr. Security Network Engineer	Engineer, Systems II	ESY2	5,760	691
Linux Administrator	Systems Administrator III	SA3	5,760	691
Database Administrator	Systems Administrator II	SA2	1,920	230
McAfee HBSS EPO* Administrator	Specialist, Information Systems Security III	SISS3	3,840	461
Software Engineer (Database)	Engineer, Computer II	EC2	1,920	0
NMCI* Service Representative	Systems Administrator I	SA1	7,680	0
VTC* Technician	Engineer, Electrical/ Electronics II	EE2	5,760	691
Customer Support Representative	Systems Administrator II	SA2	17,280	2,074
NMCI Seat Representative	Specialist, Public Affairs	SPA	24,960	2,995
MFD technician	Manager, Administrative I	MANA1	3,840	0
Network Cable Installer	Engineer, Electrical/ Electronics II	EE2	3,840	0
Administrator Support	Manager, Administrative I	MANA1	9,600	0
Information/ Inventory Technology Specialist	Specialist, Configuration MGMT I	SCM1	1,920	0
Business Analyst (NAVITAS)	Acquisition Management Support II	AMS2	5,760	231
Cellular Support	Specialist, Configuration MGMT I	SCM1	3,840	154
Senior Data Storage Administrator (Cloud Architect)	Systems Administrator III	SA3	1,920	0
OPTION YEAR 3 Total			136,320	10,983
OPTION YEAR 4				

NSWCPD Labor Category (LCAT)	eCRAFT Labor Category (LCAT)	eCRAFT Code	Hours	OT Hours
Project Manager	Manager, Program/ Project II	MANPII	1,920	0
Server Administrator (Windows Admin)	Systems Administrator III	SA3	7,680	922
Virtualization Administrator	Systems Administrator III	SA3	5,760	691
Cybersecurity Technician (IAVM Patch Manager)	Systems Administrator II	SA2	3,840	461
Software Engineer (programming)	Engineer, Computer II	EC2	5,760	0
Sr. Security Network Engineer	Engineer, Systems III	ESY3	5,760	691
Jr. Security Network Engineer	Engineer, Systems II	ESY2	5,760	691
Linux Administrator	Systems Administrator III	SA3	5,760	691
Database Administrator	Systems Administrator II	SA2	1,920	230
McAfee HBSS EPO* Administrator	Specialist, Information Systems Security III	SISS3	3,840	461
Software Engineer (Database)	Engineer, Computer II	EC2	1,920	0
NMCI* Service Representative	Systems Administrator I	SA1	7,680	0
VTC* Technician	Engineer, Electrical/ Electronics II	EE2	5,760	691
Customer Support Representative	Systems Administrator II	SA2	19,200	2,304
NMCI Seat Representative	Specialist, Public Affairs	SPA	26,880	3,226
MFD technician	Manager, Administrative I	MANA1	3,840	0
Network Cable Installer	Engineer, Electrical/ Electronics II	EE2	3,840	0
Administrator Support	Manager, Administrative I	MANA1	9,600	0
Information/ Inventory Technology Specialist	Specialist, Configuration MGMT I	SCM1	1,920	0
Business Analyst (NAVITAS)	Acquisition Management Support II	AMS2	5,760	231
Cellular Support	Specialist, Configuration MGMT I	SCM1	3,840	154
Senior Data Storage Administrator (Cloud Architect)	Systems Administrator III	SA3	1,920	0
OPTION YEAR 4 Total			140,160	11,444
Total Reg. Hours				662,400
Total OT Hours				52,612
TOTAL HOURS				715,012

*

- HBSS EPO- McAfee Host Based Security System ePolicy Orchestrator
- NAC- Network Access Control
- NAVITAS- Navy Information Technology Approval System
- NMCI- Navy Marine Corp Intranet
- VTC- Video Tele-conferencing

12.2 DON Cyberspace IT/Cybersecurity Information Assurance Functions and Personnel Requirements. The contractor shall ensure that if they have any labor categories that will be performing Information Assurance (IA) Requirements including contractors who will be in the Cybersecurity (CS) workforce, they (contractor) must identify and require the mandatory security, certifications, education, and training for EACH labor category. Reference DFARS Clause 252.239-7001, DoD 8570.01-M “Information Workforce Improvement Program”, DoD 8140.01 “Cyberspace Workforce Management”, and SECNAV M-5239.2 “Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification Manual requirements”.

Further information regarding positions that qualify as “CSWF” workforce is provided in Enclosure (1), the CSWF Tasks Outline.

Paragraph	eCRAFT Labor Category	IAT/IAM	Proficiency Level	Baseline Qualifications	Operating System/Computing Environment (OS/CE) Qualification	Continuing Professional Education (CPE) Requirements
Para 3.0	Manager, Program/ Project II	IAM	3	CISM, CISSP (or Associate), GSLC, CCISO	Directed by the Privileged Access Agreement	40 CPEs annually

Para 3.5	Systems Administrator III (Windows Admin)	IAT	3	CASP+ CE, CCNP Security, CISA, CISSP (or Associate), GCED, GCIH	Directed by the Privileged Access Agreement	40 CPEs annually
Para 3.5	Systems Administrator III (VM Admin)	IAT	3	CASP+ CE, CCNP Security, CISA, CISSP (or Associate), GCED, GCIH	Directed by the Privileged Access Agreement	40 CPEs annually
Para 3.5.8	Systems Administrator II (IAVM Mngr)	IAT	2	CCNA Security, CySA+, GICSP, GSEC, Security+ CE, SSCP	Directed by the Privileged Access Agreement	40 CPEs annually
Para 3.18	Engineer, Computer II (Software engineer-programmer)	IAT	2	CCNA Security, CySA+ **, GICSP, GSEC, Security+ CE, SSCP	Directed by the Privileged Access Agreement	40 CPEs annually
Para 3.1	Engineer, Systems III (Snr. Security Network Engineer)	IAT	3	CASP+ CE, CCNP Security, CISA, CISSP (or Associate), GCED, GCIH	Directed by the Privileged Access Agreement	40 CPEs annually
Para 3.1	Engineer, Systems II (Jr. Security Network Engineer)	IAT	2	CCNA Security, CySA+ **, GICSP, GSEC, Security+ CE, SSCP	Directed by the Privileged Access Agreement	40 CPEs annually
Para 3.2.4	Systems Administrator III (Linux Admin)	IAT	3	CASP+ CE, CCNP Security, CISA, CISSP (or Associate), GCED, GCIH	Directed by the Privileged Access Agreement	40 CPEs annually
Para 3.17	Systems Administrator II (Database Administrator)	IAT	2	CCNA Security, CySA+ **, GICSP, GSEC, Security+ CE, SSCP	Directed by the Privileged Access Agreement	40 CPEs annually
Para 3.15	Specialist, Information Systems Security III (McAfee HBSS EPO* Administrator)	IAT	3	CASP+ CE, CCNP Security, CISA, CISSP (or Associate), GCED, GCIH	Directed by the Privileged Access Agreement	40 CPEs annually

Para 3.17	Engineer, Computer II (Software Engineer (Database)	IAT	2	CCNA Security, CySA+ **, GICSP, GSEC, Security+ CE, SSCP	Directed by the Privileged Access Agreement	40 CPEs annually
Para 3.13	Systems Administrator I (NMCI Service Representative)	IAT	1	A+ CE, CCNA-Security, Network+ CE, SSCP	Directed by the Privileged Access Agreement	40 CPEs annually
Para 3.7	Engineer, Electrical/ Electronics II (VTC Technician)	IAT	2	CCNA Security, CySA+ **, GICSP, GSEC, Security+ CE, SSCP	Directed by the Privileged Access Agreement	40 CPEs annually
Para 3.13	Systems Administrator II (Customer Support Representative)	IAT	2	CCNA Security, CySA+, GICSP, GSEC, Security+ CE, SSCP	Directed by the Privileged Access Agreement	40 CPEs annually
Para 3.13	Specialist, Public Affairs (NMCI Seat Representative)	IAT	1	A+ CE, CCNA-Security, Network+ CE, SSCP	Directed by the Privileged Access Agreement	40 CPEs annually
Para 3.14.5	Specialist, Configuration MGMT I (Information/ Inventory Technology Specialist)	IAT	1	A+ CE, CCNA-Security, Network+ CE, SSCP	Directed by the Privileged Access Agreement	40 CPEs annually
Para 3.2	Systems Administrator III (Senior Data Storage Administrator-Cloud Architect)	IAT	3	CASP+ CE, CCNP Security, CISA, CISSP (or Associate), GCED, GCIH	Directed by the Privileged Access Agreement	40 CPEs annually

12.3 Key Personnel

12.3.1 The Contractor shall allow as many personnel as practicable to remain on the job to help the successor maintain the continuity and consistency of the services required by this task order in accordance with Clause 52.237-3 Continuity of Services (Jan 1991) in the basic SeaPort contract. The Contractor also shall disclose necessary personnel records and allow the successor to conduct on-site interviews with these employees. If selected employees are agreeable to the change, the Contractor shall release them at a mutually agreeable date and negotiate transfer of their earned fringe benefits to the successor.

12.3.2 In accordance with 5252.237-9106 (A) Substitution Of Personnel (PD-H05), the following labor categories are designated as the target Key Personnel for this contract. Resumes will be submitted for each category in the quantities indicated by the key category description. Target qualifications are listed below for each education and work experience qualifications for each key personnel labor category. The proposed combined expertise of all proposed key personnel shall cover at a minimum all requirements for task areas C.1-C.6 in the performance work statement.

Any labor categories that will be performing Information Assurance (IA) Requirements including contractors who will be in the Cybersecurity (CS) workforce, they (contractor) must meet the DoD 8570.01-M Cybersecurity Workforce requirements

The Contractor shall provide individuals to fill the key positions identified below:

-

1. Manager, Program/Project II (1 Resumes):

Target Education: Bachelor's degree in computer science, information technology, communications systems management or an equivalent technical degree from an accredited college or university.

Target Experience: Ten (10) years' experience in managing a team on information technology or network projects and possess knowledge in: Ethernet LANs, enterprise network architecture and design; multi-level server design; software virtualization; cloud solution and architecture; and WAN approaches. Individual should possess expertise in Microsoft Project. Management experience should demonstrate one's ability to plan, schedule, and execute projects from inception through to their successful completion within the associated time constraints. Management experience also should include hands on management of IT operations teams that include supervision, mentoring, and troubleshooting.

2. Systems Administrator III (*Windows Server Administrator*) (2 Resumes):

Target Education: Bachelor's degree in computer science, information technology, or an equivalent technical degree from an accredited college or university.

Target Experience: Seven (7) years' experience administering a Microsoft Windows domain Active Directory environment and should have extensive knowledge of and experience with installation, configuration, and integration, backups, troubleshooting and problem resolution for servers associated with an Active Directory environment.

Experience should demonstrate familiarity with Active Directory environments and Two Factor authentication for authorized system access, as well as demonstrate familiarity with application and system transfer procedures to other DoD-approved hosting facilities such as Defense Information System Agency (DISA) Computing Services Directorate (CSD) or SPAWAR System Center (SSC) Pacific (PAC) Data Center (DC).

3. Systems Administrator III (*Virtualization Administrator*) (2 Resumes):

Target Education: Bachelor's degree in computer science, information technology, or an equivalent technical degree from an accredited college or university.

Target Experience: Three (3) years' experience administering a VMware Virtual Environment, which should include extensive knowledge of and experience with installation, configuration, and integration, backups, troubleshooting and problem resolution for servers associated with a VMware Virtual Infrastructure such as ESXi and vCenter Servers. Experience should also include configuring new virtual machines (VM's) and Windows Server Operating experience.

4. Engineer, Systems III (*Sr. Security Network Engineer*) (2 Resumes):

Target Education: Bachelor's degree in information technology, computer science, or an equivalent technical degree from an accredited college or university.

Target Experience: Eight (8) years' experience in network security, demonstrating strong experience with Cisco Prime Infrastructure, understanding of IEEE 802.11 protocols, familiarity with TCP/IP (specifically Layers 3/4), and switching and routing protocols (internet standards and general architecture) and associated hardware.

Must demonstrate at time of proposal, possession of the following Certification: IAT Level III CISSP/CCNP-Routing or CCNP Security

5. Systems Administrator III (*Linux Administrator*) (2 Resumes):

Target Education: Bachelor's degree in computer science, information technology, or an equivalent technical degree from an accredited college or university.

Target Experience: Three (3) years' experience with administering Linux operating systems, specifically Red Hat Enterprise Linux. Individual should have strong communication, teamwork, and customer relational experience, and strong technical problem solving experience. This individual should have experience in security and network/distributed computing concepts, and an ability to write and maintain BASH and Perl shell scripts, in addition to experience in DHCP, DNS, and maintaining DoD STIG Compliance. Individual should demonstrate extensive knowledge of and experience with installation, configuration, and integration, backups, troubleshooting and problem resolution for servers associated with an Active Directory Domain.

6. Systems Administrator II (*Database Administrator*) (1 Resume):

Target Education: Bachelor's level degree in Computer Science or Information Systems.

Target Experience: Five (5) years professional experience in database systems administration, to include tasks such as the development, design, and maintenance of databases and/or data management systems that allow for the secure storage, query, and utilization of data. Experience should demonstrate support regarding incident management, service level management, change management, release management, continuity management, and availability management for databases and data management systems.

7. Specialist Information Systems Security III (*McAfee HBSS ePO Administrator*) (1 Resume):

Target Education: Bachelor's level degree in Computer Engineering, Computer Science, or Information Systems.

Must demonstrate at time of proposal, possession of training and/or the following Certification: at minimum, HBSS (e.g. DISA HBSS 201 Admin ePO5.1 and DISA HBSS 301 Advanced ePO5.1) and CISSP.

Target Experience: Five (5) years' professional experience in McAfee HBSS EPO administration and management having performed activities regarding the strategic planning, scheduling, implementation, and maintenance of HBSS-servers for an organization. Experience should include work with Intrusion Detection and Prevention Systems (IDS/IPS), preferably with McAfee Host Intrusion Prevention System (HIPS), McAfee Data Loss Prevention Endpoint (DLP), and/or McAfee product policy tuning.

12.4 Non-Key Personnel

Although resumes for "Non-Key Personnel" are not required, offerors must fully demonstrate their ability to provide the non-key personnel listed below who meet the requirements that follow. The Contractor shall certify in their proposal that they have these non-key personnel and provide a statement as to their ability to supply the personnel with the experience required to perform the efforts specified in the performance work statement. The Contractor shall provide individuals to fill the non-key positions identified below:

Any labor categories that will be performing Information Assurance (IA) Requirements including contractors who will be in the Cybersecurity (CS) workforce, they (contractor) must meet the DoD 8570.01-M Cybersecurity Workforce requirements

1. Systems Administrator II (*IAVM Patch Manager and Vulnerability Specialist*):

Minimum Education: Bachelor's level degree in Computer Engineering, Computer Science, or Information Systems.

Minimum Experience: Five (5) years' experience in Cybersecurity and in supporting patching and configuring Windows and Linux operating systems and third-party applications. Specifically, experience with the ACAS platform and hands on experience deploying an ACAS server and troubleshooting issues with each product, as well as the configuration of the application level for internal and customer use.

Must demonstrate at time of proposal, possession of the following Certification: DISA ACAS Certification

2. Engineer, Computer II (*Software Engineer, programming)*

Minimum Education: Bachelor's level degree in Computer, Electrical or Mathematics with field of concentration in computer science.

Minimum Experience: Three (3) years of professional experience in computer software development applying the principles and techniques of computer science, engineering, and mathematical analysis for the design, development, testing, and evaluation of software and systems that enable computers to perform their many applications.

3. Engineer, Systems II (*Jr. Security Network Engineer*):

Minimum Education: Bachelor's degree in Information Technology, Computer Science, or an equivalent technical degree from an accredited college or university.

Must possess the following certificates: IAT Level II Security+/CCNA-Routing or CCNA Security

Minimum Experience: Three (3) years' experience in network security, demonstrating strong experience with network security appliance (e.g. Cisco ASA firewall, Cisco ISE, Cisco FirePower Services), understanding of IEEE 802.11 protocols, familiarity with TCP/IP (specifically Layers 2/3), and switching and routing protocols (internet standards and general architecture) and associated hardware.

Cisco CCNA Routing or CCNA Security experience is required.

4. Engineer, Computer II (*Software Engineer, Database)*

Minimum Education: Bachelor's level degree in Computer Science, Electrical or Mathematics with field of concentration in computer science.

Minimum Experience: Three (3) years of professional experience in database engineering and development regarding the design and implementation of database systems, including the analysis of user needs and software requirements to determine feasibility of design/modification of existing or new applications within time and cost constraints.

5. Systems Administrator I *(NMCI Service Representative)*

Minimum Education: Associate's degree in computer related field.

Minimum Experience: Three (3) years' experience interfacing with business IT users. Individual shall have experience with IT service desk workflows and supporting applications including ticket management tools. Experience shall demonstrate basic troubleshooting (e.g. performed system-tests and authorized system-changes).

6. Engineer, Electrical/Electronics II (*VTC Technician and Network Communications Specialist*):

Minimum Education: Associate's degree in a computer related field.

Must demonstrate at time of proposal, possession of the following Certification Cisco Certified Network Administrator (CCNA)

Minimum Experience: Three (3) years' experience working with CISCO Video Networking, Video Teleconferencing (VTC) and Audio Visual (A/V) equipment from multiple manufactures, VTC and A/V industry standards, WAN technologies as they apply to VTC operations, developing and implementing communication tools for use between remote sites; Microsoft Office (Word, Power Point, Excel, and Outlook); and PC operations and technology.

7. Systems Administrator II (*Customer Support Representative*):

Minimum Education: Associate's degree in computer related field.

Minimum Experience: Three (3) years' experience interfacing with users who perform systems and software engineering. Individual shall have experience with IT service desk workflows and supporting applications including remote support tools and ticket management tools. Experience shall demonstrate efficient and proper record keeping of reported incidents and associated resolutions.

8. Specialist, Public Affairs (*NMCI Seat Representative*):

Minimum Education: Associate's degree in a computer related field.

Minimum Experience: Three (3) years' experience in using enterprise software systems to to interface with clients/users. Experience shall demonstrate IT inventory control, and help desk support with Microsoft Windows (i.e. Microsoft Excel, Microsoft Word) as well asAcrobat Pro.

9. Manager, Administrative I (*MFD*):

Minimum Education: Associate's degree in computer related field.

Minimum Experience: One (1) year experience interfacing with business IT users to help resolve issues and documenting IT service desk workflows and supporting applications including ticket management tools regarding multi-function devices.

10. Engineer, Electrical/Electronics II (*Network Cable Installer*):

Minimum Education: High school degree or equivalent.

Must demonstrate at time of proposal, possession of the following Certification: BICSI.

Minimum Experience: Eight (8) years' experience in installing Ethernet and fiber optic networks, network components and network interface devices. This experience shall include running, connecting, terminating, testing, and troubleshooting CAT 5e and CAT6e (STP and UTP), multi and single mode fiber optic cable, wireless, and voice systems. Individual shall have familiarity with DoD security requirements, including red/black separation and penetration protection

requirements.

11. Manager, Administrative I (*Administrative Support*)

Minimum Education: Associate's degree.

Minimum Experience: Five (5) years' experience providing administrative support. Experience in word processing, filing, tracking man-hours/time, preparing correspondence reports/forms and presentations, arranging travel, scheduling meetings and teleconferencing services. Experience with Microsoft Word, Excel, and PowerPoint. Individual should be able to develop clear, concise, and impactful PowerPoint briefings based on feedback and information available from the management team. Familiar with DoD Correspondence Manual and demonstrates advanced capabilities in Microsoft Word, Excel, and PowerPoint. Working with subject matter experts, individual must be able to draft a properly formatted standard operating procedure (SOP) document and acquire necessary approvals.

12. Specialist, Configuration MGMT I (*Information/ Inventory Technology Specialist*)

Minimum Education: Associate's degree in a computer related field.

Minimum Experience: One (1) year of professional experience in IT configuration management, inventory control, help desk support, and workflow implementation having demonstrated knowledge of policies and regulations governing those subject areas and maintaining processes to ensure compliance with those directives.

13. Acquisition Management Support II(*NAVITAS*)

Minimum Education: Associate's degree in a computer related field.

Minimum Experience: One (1) year of experience in managing Information Technology Procurement Requests (ITPRs) in IT approval work flows. Must have fundamental understanding of IT hardware, software, and authorization requirements for enterprise systems.

14. Specialist, Configuration MGMT I (*Cellular Devices Support*)

Minimum Education: Associate's degree in a computer related field.

Minimum Experience: Three (3) years of experience in cellular configuration management and is responsible for and integration of mobile devices (i.e. smartphones, cell phones, Wi-Fi cards, cellular modems) into enterprise networks. Individual should have fundamental knowledge of Apple iPhone and Android devices, and at least two (2) years of experience providing customer support to cellular device users.

15. Systems Administrator III (Cloud Solutions Architect)

Minimum Education: Bachelor's level degree in the field of computer science, information systems, or computer engineering.

Minimum Experience: Seven (7) years' experience in software engineering or IT systems architecture, of which three (3) years must demonstrate experience as a Cloud Engineer/Architect with a proven track record of cloud engagements and digital transformations (e.g. working with Azure or AWS, developing technical strategies used for rollout; and building cloud governance plans).